UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS

MATTHEW BAXTER, MARK DRISCOLL, AND RANDI TORRES IRIZARRY, on behalf of themselves and a class of similarly situated persons, Plaintiffs, v. ORACLE CORPORATION, Defendant.	**CASE NO.: 1:25-cv-00601** **CLASS ACTION COMPLAINT JURY TRIAL DEMANDED**

Plaintiffs Matthew Baxter, Mark Driscoll, and Randi Torres Irizarry, individually and on behalf of all others similarly situated ("Plaintiffs"), bring this action against Defendant Oracle Corporation ("Oracle"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class and Subclass, as defined below. Plaintiffs make the following allegations upon information and belief, the investigation of their counsel, and personal knowledge or facts that are a matter of public record.

I. INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devasting. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have grave consequences for victims for years after the actual date of the breach—with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, and/or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

[1] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, 25 S.C. LAWYER 28- 35 (May 2014), https:// https://articlegateway.com. (Last accessed June 13, 2024).

Moreover, the release disclosure, and publication of private medical information, such as diagnosis, medications and prescriptions can lead to sophisticated and costly insurance fraud, as well as embarrassment, humiliation and blackmail.

2. Defendant Oracle is the second largest Electronic Health Records ("EHR") vendor in the United States, providing EHR services to over 20% of U.S. hospitals.[2] As a major EHR provider, Oracle provides database and cloud storage and management services to hospitals and healthcare providers across the country.

3. Oracle has admitted through notice to some impacted customers that "on or around 20 February 2025, we became aware of a cybersecurity event involving unauthorized access to some amount of your Cerner data that was on an old legacy server not yet migrated to the Oracle Cloud."[3] Oracle's notice further admitted that the threat actor breached Defendant's servers sometime after January 22, 2025, accessed data that may include Electronic Health Records, and "copied data to a remote server.[4] Others have confirmed that "patient data was stolen in the attack."[5] This Data Breach (the "Data Breach") thus constitutes confidential and highly sensitive Personally Identifiable Information (PII) and Protected Health Information (PHI).

4. Even though Oracle became aware of the Data Breach as early as February 20, 2025, it has not publicly disclosed the incident and has informed hospitals that Oracle will not notify patients directly.[6] On information and belief, Oracle has made exceptionally limited efforts to alert the potentially millions of consumers and patients whose private information was exfiltrated. Instead,

---

[2] *See* Maggy Bobek Tieche, *Most Common Hospital HER Systems By Market Share*, Definitive Healthcare (Jan. 10, 2024), https://www.definitivehc.com/blog/most-common-inpatient-ehr-systems (last accessed Apr. 2, 2025).
[3] See Jordon Sollof, *US Patient Data Reportedly Stolen Following Oracle Health Breach*, Digital Health (Apr. 2, 2025), https://www.digitalhealth.net/2025/04/us-patient-data-reportedly-stolen-following-oracle-health-breach/ (last accessed Apr. 2, 2025).
[4] *Id.*
[5] *See* Lawrence Abrams, *Oracle Health Breach Compromises Patient Data at US Hospitals*, Bleeping computer (Mar. 28, 2025), https://www.bleepingcomputer.com/news/security/oracle-health-breach-compromises-patient-data-at-us-hospitals/ (last visited Apr. 2, 2025).
[6] *Id*.

Oracle maintains that it is the responsibility of its many customer healthcare providers to send notice to victims of the Breach.[7]

5. Oracle is fantastically wealthy and is the twenty-first largest company in the world by market capitalization.[8] Oracle received $53,000,000,000 in total revenue in fiscal year 2024 and had $10,454,000,000 in cash and cash equivalents on hand on May 31, 2024.[9] Oracle could easily have allocated a small portion of their profits toward cybersecurity and prevention to forestall and prevent the Data Breach. But Oracle chose profits over protection of patients' most sensitive PII and PHI. As a result of the Data Breach, through which their PII and PHI was compromised, disclosed, and obtained by unauthorized third parties, Plaintiffs and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. And they must make family and close friends aware that personal health information about Class Members could be used in fraud and phishing attempts targeting their friends and families. Consequently, Plaintiffs and the other Class Members will incur ongoing out-of-pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft and other fraudulent behavior.

6. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose private information was accessed during the Data Breach.

II. JURISDICTION, VENUE, AND CHOICE OF LAW

7. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §

[7] *Id.*
[8] *See* https://companiesmarketcap.com/ (last visited Apr. 2, 2025).
[9] *See Oracle Announces Fiscal 2024 Fourth Quarter and Fiscal Full Year Financial Results*, PR Newswire (Jun. 11, 2024), https://www.prnewswire.com/news-releases/oracle-announces-fiscal-2024-fourth-quarter-and-fiscal-full-year-financial-results-302169918.html (last visited Apr. 2, 2025).

1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than the Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

8. The Court has personal jurisdiction over this action because Defendant maintains its principal place of business in Austin, Texas, in this District, they have sufficient minimum contacts with this District, and has purposefully availed themselves of the privilege of doing business in this District such that they could reasonably foresee litigation being brought in this District.

9. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendant's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

A. PLAINTIFF MATTHEW BAXTER

10. Plaintiff Matthew Baxter is a citizen of and is domiciled in the state of Oklahoma.

11. Plaintiff is a consumer and patient who has obtained products or services from one or more of the healthcare providers to whom Defendant provides products and services.

12. Plaintiff provided confidential and sensitive PII and PHI to one or more of the healthcare providers to whom Defendant provide products and services and those companies, in turn, provided Plaintiff's PII and PHI to Defendant, in connection with Defendant's provision of their services. On information and belief, Defendant obtained and continues to maintain Plaintiff's PII and PHI and have a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

13. Plaintiff Baxter would not have entrusted his PII and PHI to Defendant had he known that Defendant failed to maintain adequate data security.

14. On or about April 15, 2025, Plaintiff Baxter discovered that his information was

likely compromised in the Data Breach.

15. Plaintiff subsequently spent substantial time taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself from data breaches, and reviewing his financial and medical accounts for fraud or suspicious activity. He now plans to spend several hours a month checking account statements for irregularities.

16. As a result of the Data Breach and the release of his PHI and PII, which he expected Defendant to protect from disclosure, Plaintiff has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PHI and PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

B. PLAINTIFF MARK DRISCOLL

17. Plaintiff Mark Driscoll is a citizen of and is domiciled in the state of Washington.

18. Plaintiff is a consumer and patient who has obtained products or services from one or more of the healthcare providers to whom Defendant provides products and services.

19. Plaintiff provided confidential and sensitive PII and PHI to one or more of the healthcare providers to whom Defendant provide products and services and those companies, in turn, provided Plaintiff's PII and PHI to Defendant, in connection with Defendant's provision of its services. On information and belief, Defendant obtained and continues to maintain Plaintiff's PII and PHI and have a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

20. Plaintiff Driscoll would not have entrusted her PII and PHI to Defendant had he known that Defendant failed to maintain adequate data security.

21. On or about April 15, 2025, Plaintiff Driscoll discovered that his information was likely compromised in the Data Breach.

22. Plaintiff subsequently spent substantial time taking action to mitigate the impact of

the Data Breach, including researching the Data Breach, researching ways to protect himself from data breaches, freezing his credit, changing his debit and credit cards, and reviewing his financial and medical accounts for fraud or suspicious activity. He now plans to spend several hours a month checking account statements for irregularities.

23. As a result of the Data Breach and the release of his PHI and PII, which he expected Defendant to protect from disclosure, Plaintiff has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PHI and PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

C. PLAINTIFF RANDI TORRES IRIZARRY

24. Plaintiff Randi Torres Irizarry is a citizen of and is domiciled in the state of Missouri.

25. Plaintiff is a consumer and patient who has obtained products or services from one or more of the healthcare providers to whom Defendant provides products and services.

26. Plaintiff provided confidential and sensitive PII and PHI to one or more of the healthcare providers to whom Defendant provide products and services and those companies, in turn, provided Plaintiff's PII and PHI to Defendant, in connection with Defendant's provision of their services. On information and belief, Defendant obtained and continues to maintain Plaintiff's PII and PHI and have a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

27. Plaintiff Irizarry would not have entrusted his PII and PHI to Defendant had he known that Defendant failed to maintain adequate data security.

28. On or about the week of April 6, 2025, Plaintiff Irizarry experienced medical identity theft regarding a $1,200.00 medical procedure that occurred in a distant state he has not recently visited. Plaintiff Irizarry was sent to collections over this fraudulent debt and has spent and will continue to spend substantial time, money, and effort to protect against this and other future

fraudulent activity.

29. Plaintiff subsequently spent substantial time taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself from data breaches, and reviewing his financial and medical accounts for fraud or suspicious activity. He now plans to spend several hours a month checking account statements for irregularities.

30. As a result of the Data Breach and the release of his PHI and PII, which he expected Defendant to protect from disclosure, Plaintiff has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PHI and PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

D. DEFENDANT ORACLE

31. Defendant Oracle Corp. is a Delaware corporation with its principal place of business located at 2300 Oracle Way Austin, Texas, 78741.

IV. FACTUAL BACKGROUND

A. DEFENDANT FAILED TO ADEQUATELY PROTECT CUSTOMER DATA, RESULTING IN THE DATA BREACH.

32. In the course of its business, Defendant collects names, phone numbers, Social Security numbers, physical addresses, driver's license information, insurance, and medical information from their customers and the customers of their customers. They also maintain medical records subject to the requirements and standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

33. As a condition of providing services, Defendant receives, creates, and handles the PII and PHI of Plaintiffs and Class Members.

34. Plaintiffs and Class Members must provide Defendant with their sensitive and confidential PII and PHI in order to receive healthcare services. Plaintiffs reasonably expected that Defendant would safeguard their highly sensitive information and keep it confidential.

35. Due to the sensitivity of the PII and PHI that Defendant handle, Defendant is aware of the critical responsibility to safeguard this information—and, therefore, how devastating its theft is to individuals whose information has been stolen.

36. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII and PHI, Defendant assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

37. Despite the existence of these duties, Defendant failed to implement reasonable data security measures to protect the information with which it was entrusted and ultimately allowed nefarious third-party hackers to compromise Plaintiffs' and Class Members' PII and PHI.

38. While some Class Members received a letter explaining what happened, not everyone whose data was stolen has been notified. There are likely millions of consumers who do not yet know that their information was impacted by this data breach.

B. DEFENDANT WAS WELL AWARE OF THE NEED TO TAKE SPECIAL CARE WITH CONSUMERS' PII, PHI AND MEDICAL INFORMATION.

39. Defendant claims to maintain protected information in compliance with HIPAA requirements.[10]

40. Defendant made these representations concerning securing consumers PII and PHI because they knew and understood the severe consequences of losing this data.

41. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (Personal Information)" so that these companies can take

[10] *See* https://docs.oracle.com/en/industries/insurance/health-insurance-components/policies-3.21.2/security/hipaa-compliance/oracle-and-hipaa.html (last visited Apr. 2, 2025).

the necessary precautions to thwart such attacks.[11]

42. The healthcare industry has become a rich target for hackers: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[12] "The IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end- of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[13]

43. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[14] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

C. ORACLE FAILED TO COMPLY WITH REGULATORY GUIDANCE AND INDUSTRY-STANDARD CYBERSECURITY PRACTICES.

44. Defendant's data security failure stems from its failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII and PHI.

45. At least twenty-four states have enacted laws addressing data security practices that require that businesses that own, license or maintain PII to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access.

---

[11] Reuters, FBI warns healthcare firms they are targeted by hackers, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last accessed June 13, 2024).

[12] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/ solutions/healthcare/healthcare-is- the-biggest-target-for-cyberattacks/ (last accessed June 13, 2024).

[13] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names.

[14] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last accessed June 13, 2024).

46. Defendant also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

47. The FTC recommends:

- limiting access to customer information to employees who have a business reason to see it;
- keeping customer information in encrypted files provides better protection in case of theft;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;
- using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,
- monitoring activity logs for signs of unauthorized access to customer information.[15]

48. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[16]

49. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[17]

---

[15] Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions- customer-information-complying (last accessed June 13, 2024).
[16] Federal Trade Commission, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed June 13, 2024).
[17] Federal Trade Commission, *Protecting PII: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last accessed June 13, 2024).

The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

50. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

51. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

54. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[18] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[19]

55. On October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[20] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[21]

56. Defendant was aware of its obligations to protect customers' PII, PHI and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access. In this case, Defendant was at all times fully aware of the obligation to protect the PII and PHI of Defendant's customers because of their status as one of the largest EHR vendors in the nation. Defendant was also aware of the significant repercussions if they failed to do so because Defendant collected PII and PHI from millions of consumers and knew that this PII and PHI, if hacked, would result in injury to consumers, including Plaintiffs and Class Members.

57. Based upon the known details of the Data Breach and how it occurred, Defendant also failed to fully comply with industry-standard cybersecurity practices, including, but not limited

---

[18] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last accessed June 13, 2024).
[19] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last accessed June 13, 2024).
[20] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last accessed June 13, 2024).
[21] *Id*.

to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, and intrusion detection and prevention.

D. DEFENDANT FAILED TO COMPLY WITH HIPAA'S DATA SECURITY REQUIREMENTS.

58. Defendant recognizes it is covered by HIPAA,[22] and is covered by HIPAA (see 45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule.[23] These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

59. HIPAA prohibits unauthorized disclosures of "protected health information" and it requires that Defendant implement appropriate safeguards for this information. HIPAA requires that entities covered by its rules, including Defendant, provide notice of a breach of unsecured protected health information—i.e., non-encrypted data—without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

60. Following a data breach at a HIPAA covered entity, the HIPAA Omnibus Rule dictates it "must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported." The four- factor risk assessment includes:

a) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers);

b) the recipient of the PHI;

c) whether the PHI was actually acquired or viewed; and,

d) the extent to which the risk that the PHI was compromised has been mitigated

[22] *See* Oracle Health Insurance Enterprise Policy Administration, Security Guide, https://docs.oracle.com/en/industries/insurance/health-insurance-components/policies-3.21.2/security/hipaa-compliance/oracle-and-hipaa.html (last visited Apr. 3, 2025).

[23] 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[24]

61. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

62. Defendant failed to comply with these HIPAA requirements and, indeed, its own Privacy Practices.[25] Defendant did not:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiff's and the Class Members' Personal Information;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. §

[24] 78 Fed. Reg. 5641-46; see also 45 C.F.R. § 164.304.
[25] *See* Oracle General Privacy Policy, https://www.oracle.com/legal/privacy/privacy-policy/#:~:text=Oracle%20has%20implemented%20appropriate%20technical,other%20forms%20of%20unlawful%20processing (last visited

164.306(a)(3);

h) Take safeguards to ensure that Defendant's business associates adequately protect protected health information;

i) Properly send timely notice to Plaintiffs and the Class Members pursuant to 45 C.F.R. §§ 164.400-414;

j) Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

k) Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. §164.530(b).

E. THE DATA BREACH PUTS PLAINTIFFS AND CLASS MEMBERS AT INCREASED RISK OF FRAUD AND IDENTITY THEFT.

63. Defendant's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII and PHI stolen in the Data Breach—names, addresses, zip codes, phone numbers, email addresses, dates of birth, Social Security Numbers, and health information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs and Class Members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

64. There is little doubt that consumers PII and PHI from the Data Breach will be circulating on the dark web, as it is highly valuable. Malicious actors use PII and PHI to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII and PHI to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."[26]

65. Further, identity thieves often wait months or years to use PII obtained in data

[26] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiffs' and Class Members' data may have been compromised in other data breaches, the fact that the Breach centralizes the PII and PHI and identifies the victims as Defendant's customers materially increases the risk to Plaintiffs and the Class.

66. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[27] Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiffs will therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach. In other words, Plaintiffs and Class Members have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Data Breach.

67. Plaintiffs and Class Members have also realized harm in the lost or reduced value of their PII. Defendant admits the PII compromised in the Breach is valuable. Defendant's revenues are predicated on Defendant's collection, retention, and use of Plaintiffs' PII and PHI. Plaintiffs' PII is not only valuable to Defendant, but Plaintiffs also place value on their PII based on their understanding that their PII is a financial asset to companies who collect it.[28]

68. Plaintiffs and Class Members have also been harmed and damaged in the amount of

[27] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (2007), https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last accessed June 13, 2024).

[28] *See, e.g.*, Ponemon Institute, LLC, *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at $55.70), available at https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us- european-and-japanese-consumers.html.

the market value of the hacker's unauthorized access to Plaintiffs' PII and PHI that was permitted without authorization by Defendant. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

69. Moreover, Plaintiffs and Class Members value the privacy of this information and expect Defendant to allocate enough resources to ensure it is adequately protected. Plaintiffs and Class Members would not have done business with Defendant, or Defendant's customers, provided their PII and PHI, or paid the same prices for the services of Defendant's customers' goods and services had they known Defendant did not implement reasonable security measures to protect their PII.[29] Customers reasonably expect that the payments they make to Defendant, its customer healthcare providers, and those made on their behalf through government programs and insurance, incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiffs and Class Members did not receive the benefit of their bargain with Defendant, or Defendant's healthcare customers, because they paid for services they expected but did not receive.

70. Given Defendant's failure to protect their PII and PHI, Plaintiffs and Class Members have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII and PHI remains in Defendant's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

[29] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last accessed June 13, 2024) (noting approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less PII to organizations that suffered a data breach).

71. In sum, Plaintiffs and Class Members were injured as follows: (i) theft of their PII and PHI and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII and PHI; (iii) loss of value of their PII and PHI; (iv) the lost value of unauthorized access to Plaintiffs' and Class Members' PII and PHI permitted by Defendant; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; (vi) Defendant's retention of profits attributable to Plaintiff's and Class Members' PII and PHI that Defendant failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out- of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to Defendant for goods and services purchased, as Plaintiffs reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII and PHI, which was not the case; and (x) nominal damages.

V. CLASS ACTION ALLEGATIONS

72. Plaintiffs bring this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed nationwide class (the "Class"), defined as:

> All natural persons in the United States whose Personally Identifiable Information and/or Protected Health Information was compromised as a result of the Data Breach.

73. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Class or identity of the Class Members, since such information is in the exclusive control of Defendant. Nevertheless, the Class encompasses at least millions of individuals dispersed throughout the United States. The number of Class Members is so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendant.

74. **Commonality and Predominance:** This action involves common questions of law

and fact which predominate over any question solely affecting individual Class Members. These common questions include:

a. whether Defendant engaged in the conduct alleged herein;
b. whether Defendant had a legal duty to use reasonable security measures to protect Plaintiff's and Class Members' PII and PHI;
c. whether Defendant violated HIPAA;
d. whether Defendant timely, accurately, and adequately informed Plaintiffs and Class Members that their PII and PHI had been compromised;
e. whether Defendant breached its legal duty by failing to protect the PII and PHI of Plaintiffs and Class Members;
f. whether Defendant acted reasonably in securing the PII and PHI of Plaintiffs and Class Members;
g. whether Plaintiffs and Class Members are entitled to injunctive relief; and
h. whether Plaintiffs and Class Members are entitled to damages and equitable relief.

75. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendant's substantially uniform misconduct, as described above. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other members of the Class that they represent, and there are no defenses or legal theories that are unique among the Plaintiffs. The claims of Plaintiffs and Class Members arise from the same operative facts and are based on the same legal theories.

76. **Adequacy:** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Class they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs intend to prosecute this action vigorously. The Class's interest will be fairly and adequately protected by Plaintiffs and their counsel.

77. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiffs and other

Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be virtually impossible for the Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not: individualized litigation creates potential for inconsistent or contradictory judgments, increases the delay and expense to the parties, and increases the expense and burden to the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by this Court.

VI. CAUSES OF ACTION

COUNT ONE
NEGLIGENCE

78. Plaintiffs reallege and incorporate by reference paragraphs 1-77 as if fully set forth herein.

79. Defendant owed a duty to Plaintiffs and Class Members, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures, and practices to ensure that Plaintiffs' and Class Members' information was adequately secured from unauthorized access.

80. Defendant's Privacy Policies acknowledged Defendant's duty to adequately protect Plaintiffs' and Class Members' PII and PHI.

81. Defendant is covered by HIPAA (see 45 C.F.R. § 160.102) and, as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part

160 and Part 164, Subparts A and C.

82. Defendant owed a duty to Plaintiffs and Class Members to implement administrative, physical, and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and Class Members' PII and PHI.

83. Defendant also had a duty to only maintain PII and PHI that was needed to serve customer needs.

84. Defendant owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and PHI.

85. Defendant also had independent duties under Plaintiffs' and Class Members' state laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and PHI, and promptly notify them about the Data Breach.

86. Defendant had a special relationship with Plaintiffs and Class Members as a result of being entrusted with their PII and PHI, which provided an independent duty of care. Plaintiffs' and Class Members' willingness to entrust Defendant with their PII and PHI was predicated on the understanding that Defendant would take adequate security precautions. Moreover, Defendant was capable of protecting its networks and systems, and the PII and PHI it stored on them, from unauthorized access.

87. Defendant breached their duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiffs' and Class Members' PII and PHI, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and PHI.

88. But for Defendant's breach of duties, including the duty to use reasonable care to protect and secure Plaintiffs' and Class Members' PII and PHI, Plaintiffs' and Class Members' PII and PHI would not have been accessed by unauthorized parties.

89. Plaintiffs and Class Members were foreseeable victims of Defendant's inadequate data security practices. Defendant knew or should have known that a breach of its data security systems would cause damage to Plaintiffs and Class Members.

90. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII and PHI would result in unauthorized access to Defendant's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' PII and PHI.

91. As a result of Defendant's negligent failure to prevent the Data Breach, Plaintiffs and Class Members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII and PHI has also diminished the value of the PII and PHI.

92. The harm to Plaintiffs and Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of the aforementioned duties.

93. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

94. Plaintiffs reallege and incorporate by reference paragraphs 1-77 as if fully set forth herein.

95. Under the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard

Plaintiffs' and Class Members' PII.

96. In addition, under state data security statutes, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

97. Defendant breached these duties to Plaintiffs and Class Members, under the FTCA and the state data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

98. Defendant is covered by HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. HIPAA prohibits unauthorized disclosures of "protected health information." which includes the information at issue here.

99. Plaintiffs and Class Members were foreseeable victims of Defendant's violations of the FTCA, HIPAA and state data security statutes. Defendant knew or should have known that the failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and Class Members.

100. Defendant's failure to comply with the applicable laws and regulations constitutes negligence *per se.*

101. But for Defendant's violation of the applicable laws and regulations, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

102. As a result of Defendant's failure to comply with applicable laws and regulations, Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to

guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft.

103. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

104. The harm to Plaintiffs and the Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of the applicable laws and regulations.

105. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT THREE
GROSS NEGLIGENCE

106. Plaintiffs reallege and incorporate by reference paragraphs 1-77 as if fully set forth herein.

107. Plaintiffs and Class Members entrusted Defendant with highly-sensitive and inherently personal private data subject to confidentiality laws.

108. In requiring, obtaining and storing Plaintiffs' and Class Members' PII and PHI, Defendant owed a duty of reasonable care in safeguarding the PII and PHI.

109. Defendant's networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiffs' and Class Members' PII and PHI were secured from unauthorized access.

110. Defendant's networks, systems, protocols, policies, procedures, and practices, as described above, were not reasonable given the sensitivity of the Plaintiffs' and Class Members' private data and the known vulnerabilities of Defendant's systems.

111. Defendant did not comply with state and federal laws and rules concerning the use and safekeeping of this private data.

112. Upon learning of the Data Breach, Defendant should have immediately disclosed the Data Breach to Plaintiffs and Class Members, credit reporting agencies, the Internal Revenue Service, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiffs and Class Members as a result of the Data Breach.

113. Despite knowing its networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiffs' and Class Members' PII and PHI were secured from unauthorized access, Defendant ignored the inadequacies and was oblivious to the risk of unauthorized access it had created.

114. Defendant's behavior establishes facts evidencing a reckless disregard for Plaintiffs' and Class Members' rights.

115. Defendant, therefore, was grossly negligent.

116. Defendant's negligence also constitutes negligence per se.

117. The negligence is directly linked to injuries.

118. As a result of Defendant's reckless disregard for Plaintiffs' and Class Members' rights by failing to secure their PII and PHI, despite knowing its networks, systems, protocols, policies, procedures, and practices were not adequately designed, implemented, maintained, monitored, and tested, Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII and PHI has also diminished the value of the PII and PHI.

119. The harm to Plaintiffs and the Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of the applicable laws and regulations.

120. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT FOUR
BREACH OF IMPLIED CONTRACTS

121. Plaintiffs reallege and incorporate by reference paragraphs 1-77 as if fully set forth herein.

122. Plaintiffs and Class Members were required to provide their PII and PHI to obtain services from Defendant or Defendant's customers. Plaintiffs and Class Members entrusted their PII and PHI to Defendant through Defendant's customers in order to obtain services from them.

123. By providing their PII and PHI, and upon Defendant's acceptance of such information, Plaintiffs and Class Members on one hand, and Defendant on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the services provided, whereby Defendant was obligated to take reasonable steps to secure and safeguard that information.

124. Defendant had an implied duty of good faith to ensure that the PII and PHI of Plaintiffs and Class Members in its possession was only used in accordance with their contractual obligations.

125. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and to comply with industry standards and state laws and regulations for the security of this information, and Defendant expressly assented to these terms in its Privacy Policies as alleged above.

126. Under these implied contracts for data security, Defendant was further obligated to

provide Plaintiffs and all Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI.

127. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant and Defendant's customers, including paying for the services provided by Defendant or Defendant's customers and/or providing the PII and PHI required by Defendant.

128. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII and PHI, resulting in the Data Breach. Defendant unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members.

129. Further, on information and belief, Defendant has not yet provided Data Breach notifications to some affected Class Members who may already be victims of identity fraud or theft, or are at imminent risk of becoming victims of identity theft or fraud, associated with the PII or PHI that they provided to Defendant. These Class Members are unaware of the potential source for the compromise of their PII and PHI.

130. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

131. As a result of Defendant's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value as compared to the secure services they paid for. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

132. Neither Plaintiffs, nor Class Members, nor any reasonable person would have provided their PII and PHI to Defendant had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures.

133. As a result of Defendant's breach, Plaintiffs and Class Members have suffered actual

damages resulting from theft of their PII and PHI, as well as the loss of control of their PII and PHI, and remain in imminent risk of suffering additional damages in the future.

134. As a result of Defendant's breach, Plaintiffs and the Class Members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII and PHI. As a result, Plaintiffs and the Class Members have suffered actual identity theft and the ability to control their PII and PHI.

135. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendant's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT FIVE
UNJUST ENRICHMENT

136. Plaintiffs reallege and incorporate by reference paragraphs 1-77 as if fully set forth herein.

137. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for services received.

138. Defendant collected, maintained, and stored the PII and PHI of Plaintiffs and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by Plaintiffs and Class Members.

139. The money that Plaintiffs and Class Members paid to Defendant or Defendant's customers should have been used to pay, at least in part, for the administrative costs and implementation of data management and security. Defendant failed to implement—or adequately implement—practices, procedures, and programs to secure sensitive PII and PHI, as evidenced by the Data Breach.

140. As a result of Defendant's failure to implement security practices, procedures, and

programs to secure sensitive PII and PHI, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiffs and Class Members paid for, and the services they received without reasonable data privacy.

141. Under principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members because Defendant failed to implement the data management and security measures that are mandated by industry standards and that Plaintiffs and Class Members paid for.

142. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by Defendant. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendant traceable to Plaintiffs and the Class.

COUNT SIX
DECLARATORY JUDGMENT

143. Plaintiffs reallege and incorporate by reference paragraphs 1-77 as if fully set forth herein.

144. Plaintiffs and the Class have stated claims against Defendant based on negligence, negligence per se and gross negligence, and violations of various state and federal statutes.

145. Defendant failed to fulfill its obligations to provide adequate and reasonable security measures for the PII and PHI of Plaintiffs and the Class, as evidenced by the Data Breach.

146. As a result of the Data Breach, Defendant's system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII and PHI of Plaintiffs and the Class going forward.

147. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide reasonable data security measures to protect the PII and PHI of Plaintiffs and the Class. Defendant maintains that its security measures were—and still are—

reasonably adequate and denies that it previously had or have any obligation to implement better safeguards to protect the PII and PHI of Plaintiffs and the Class.

148. Plaintiffs seek a declaration that Defendant must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII and PHI of Plaintiffs and the Class. Specifically, Plaintiffs and the Class seek a declaration that Defendant's existing security measures do not comply with their obligations, and that Defendant must implement and maintain reasonable security measures on behalf of Plaintiffs and the Class to comply with their data security obligations.

VII. PRAYER FOR RELIEF

Plaintiff, on behalf of themselves and on behalf of the proposed Class and Subclasses, request that the Court:

a. Certify this case as a class action, appoint Plaintiffs as class representative, and appoint Plaintiffs' Counsel as Class Counsel for Plaintiffs to represent the Class;

b. Find that Defendant breached its duty to safeguard and protect the PII and PHI of Plaintiffs and Class Members that was compromised in the Data Breach;

c. Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution, and disgorgement;

d. Award equitable, injunctive, and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: April 21, 2025

Respectfully submitted,

By: */s/ W. Mark Lanier*

W. Mark Lanier
TX Bar No. 11934600
THE LANIER LAW FIRM, P.C.
10940 W. Sam Houston Pkwy N.
Suite 100
Houston, Texas 77064
T: (713) 659-5200
F: (713) 659-2204
mark.lanier@lanierlawfirm.com

COTCHETT, PITRE & MCCARTHY LLP
Thomas E. Loeser*
Karin B. Swope*
Jacob M. Alhadeff*
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 970-8181
Fax: (650) 697-0577
tloeser@cpmlegal.com
kswope@cpmlegal.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
Gary M. Klinger*
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
T: (866) 252-0878
gklinger@milberg.com

**Pro Hac Vice Forthcoming*

Counsel for Plaintiffs and the Proposed Class